Public Randomness

Goals:
- Investigate the value of public randomness as a public good.
- Foster applications that use public randomness with the NIST format.

Sources of public randomness:
- Natural: earthquakes, solar storms, fire patterns, ..., quantum processes
- Social: lottery results, stock market prices, twitter feeds, ..., blockchains
- Custom: cryptographic Randomness Beacons (like the NIST Beacon)

A Randomness Beacon

- Periodically publishes a randomness pulse
- Each pulse contains a fresh sequence of 512 random bits
- The pulses are indexed, have a timestamp and a digital signature
- Past pulses are publicly available
- The sequence of pulses forms a hash chain

NIST has a project about Interoperable Randomness Beacons, with four tracks:
A. Beacons Reference: promote a reference for randomness beacons;
B. NIST Beacon: maintain a NIST Beacon implementation;
C. External Beacons: promote the deployment of other Beacons by multiple organizations;
D. Uses of public randomness: foster applications that use beacon-issued randomness.

Generic applications

Public auditability

- Setting: You need to make a random choice from a set \{C_1, ..., C_n\} of possibilities.
- Challenge: At a later time you would like to prove to a judge that all choices were equally likely when you made the selection.
- Solution: Cryptographic commitments, time stamps, and a public source of randomness are enough to solve your problem.

Quality control

- Setting: Randomized sampling is used for quality control in manufacturing processes. The process can be compromised if the random samples are chosen by a worker in the factory floor (or insiders in general).
- Application: With public randomness, a phone app can instead do the sampling. The factory can also keep an audit trail for later verification.

Use-case 1: Random officials for financial audit

- Setting: The government of Chile selects random public officials for financial audits. Each official has a risk score based on public and private information (e.g., stock holdings of spouses). The probability of selection should be proportional to the risk score.
- Challenge: Enable public auditability of the selection, along with privacy of the data used to compute the score.
- Solution: Use public randomness from a beacon along with zero-knowledge proofs. Note: Chile has implemented a Beacon following the NIST reference for randomness beacons.

Use-case 2: Randomized clinical trials

- Example setting: a placebo-controlled clinical trial assigns patients to either the treatment group or the control group.
- Goal: After the study, it is possible to convince others that the trial was properly randomized.

Prepare clinical trial

Trial id: 123
Created: 5 pm
Will use: pulse issued at 6 pm
List patients:
1. Ann
2. Bob
3. Cai
4. Dan
5. Eve
6. Fae

Obtain verifiably random groups for clinical trial

Time flow of a clinical trial protected by the Beacon

Assign

Others example use-cases

Random judges for court cases

- For years, New Orleans has been struggling with a problem referred to as forum shopping: prosecutors were being accused of gaming the court system so as to have friendly judges assigned to certain cases.
- The Criminal District Court judges saw it useful to implement random assignment of judges to cases. Real-life constraints makes this a non-trivial problem. NIST could help if we get a full specification of the problem.

Eliminating bias in randomized security checks

- Setting: “You have been randomly chosen for additional security screening.”
- Goal: Allow individuals to confirm that the selection was really random.

Use-case 3: Legal metrology

An application motivated by INMETRO (Brazil), using a Beacon with the NIST reference

- Goal: Improve metrological inspections through public randomness
- Challenge: Gas pumps and other instruments are subject to malicious firmware replacement and counterfeit
- Solution: Authentication checking uses public randomness for metrological verifications

The Protocol

- Model Registration: The metrology authority registers the approved gas pump model and publishes the digital fingerprint (hash H) of its secret software. The hash H is obtained through a function F that takes the software (binary code) as input.

The Interoperable Randomness Beacons Project: beacon@nist.gov

Poster produced for: NIST-ITL Science Day 2019 — November 06, 2019 (Gaithersburg, USA)